# NOD 32
antivirus system

# User's Guide

# NOD 32
antivirus system

# User's Guide

**Eset, LLC**
1317 Ynez Place, Ste C
Coronado, CA 92118
www.nod32.com

**For Sales and Technical Support (US and Canada):**
Tel: (619) 437-7037

**Online purchase:**
http://www.nod32.com/purchase/purchase_usa.htm

**Sales:**
sales@eset.com

**Technical Support:**
http://www.nod32.com/support/support.htm

**For Sales and Technical Support (outside US and Canada):**
http://www.nod32.com/worldwide

# Conventions Used in this Manual


**NOTE:** Notes indicate important supplemental information that helps you make better use of the program.


**IMPORTANT!** Text marked as "Important" indicates a warning, or other critical information, that may help you avoid damage or loss of data.

**This document uses the following typographic conventions:**

**Enter**
Used for key names, screen elements, and for options you are told to select.

`Nodnten.cab`
Used for file and program names, and for screen messages.

**`C:\type.exe`**
Used for text that must be typed exactly as shown.

# Table of Contents:

# 1 • Installation

## 1.1 Minimum System Requirements

Make sure the computer where you plan to install NOD32 meets the minimum system requirements:

- **CPU:** 386 or higher (Pentium recommended)
- **Space:** 30MB free disk space, 32MB of RAM (64 recommended).
- **Display Adaptor**: VGA or higher resolution video card. (SVGA 800 x 600 Recommended).

If another antivirus program has previously been installed on your system, its resident (or on-access) scanner may conflict with NOD32. Usually, resident scanners will display an icon in the system tray (the area of the taskbar near the system clock). We recommend removing any other antivirus software (including older versions of NOD32) before installing NOD32, version 2, to avoid serious problems.

## 1.2 Getting the Software

The following describes installation from either a CD, or from a file downloaded from the Internet:

- To install from a NOD32 CD, simply insert the CD into the drive. If setup does not begin automatically, you will need to run the file `Setup.exe` from the CD's root directory. Operating System detection is done automatically, so the correct version of NOD32 will be installed.
- To install from an Internet file, first download the correct file from the NOD32 website (*www.nod32.com/download*) using the **username** and **password** provided by your NOD32 vendor. Be sure to get the right version for your operating system (e.g. "Windows 95/98/Me"

or “Windows NT/2000/XP”). When prompted to save or open the file, select save, and choose a location to store the file. Once downloading is complete, start installation by opening the file you just downloaded. To open the file, double-click the icon of the file.

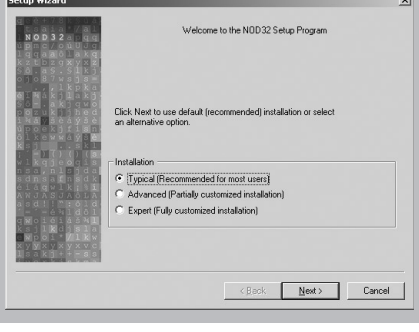
First, the setup files need to be extracted from the installation archive. The setup program will prompt you for a folder to extract to. Use the default unless you have a specific reason to change it. Click **Extract** to continue.


The installation process will check for an older version of NOD32 and if found, it will prompt you to use the settings from the current version. This will automatically enter your Update username and password, and other settings into the new version. If you don’t want to keep the current settings, clear this box.

## 1.3 Installation Type

If you’re not upgrading from a previous version, or if you didn’t choose to re-use your current settings, choose the installation type:

- **Typical** - this is the recommended type for most users.
- **Advanced** - useful for network administrators.
- **Expert** - manually set all installation options.

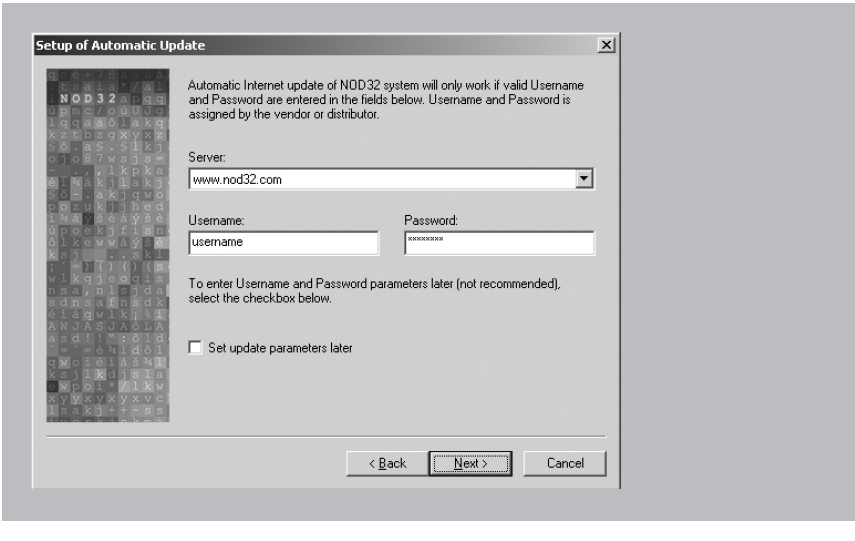


**NOTE:** This guide describes the "Typical" installation type. For advanced computer users and system administrators, "Appendix B: Installation Types" shows a summary of options available in the other installation types.

Next, read and choose to accept or decline the Software License Agreement. Note that if you decline, installation cannot proceed.

## 1.4 Username and Password

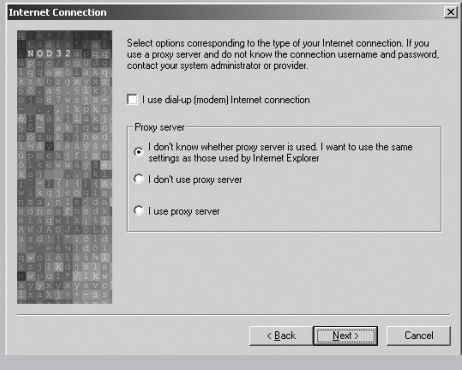
On the next screen, enter the username and password provided to you by your NOD32 vendor. Pay close attention to capital and lower-case letters,




these must be entered exactly as provided to you (i.e.: both username and password are case-sensitive). Using the "copy and paste" method is highly recommended. Don't check the **"provide parameters later"** box, unless you don't want to enter your username and password during installation. (This is not recommended, since it is very important that your computer is able to get the latest virus signatures and program updates from Eset's servers as soon as installation is complete.)

## 1.5 Internet Connection

The Internet connection settings let your computer get updates in the most efficient way, depending on the type of connection you have. Dial-up or




modem users should check the **"I use dial-up..."** box, while most cable, LAN, and other broadband users will leave this box unchecked if they have an "always on" connection to the Internet.

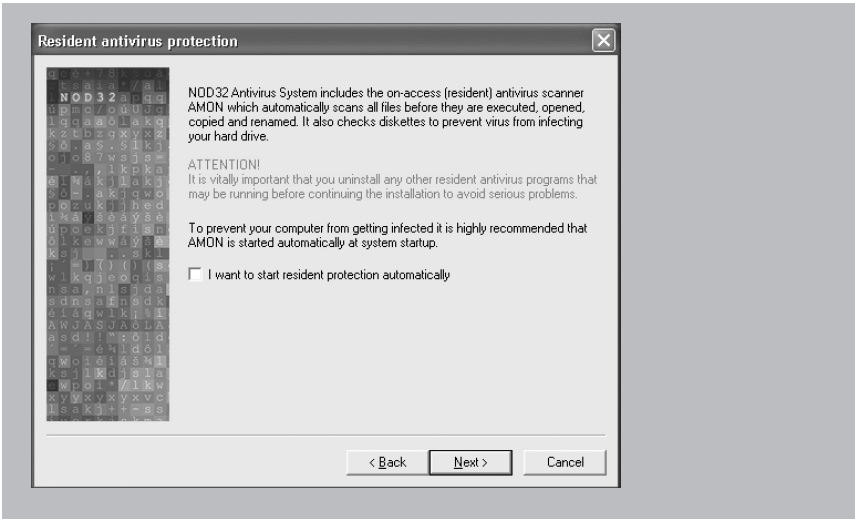
**NOTE:** Some Internet connection services require you to start your Internet connection manually after your computer is up and running. This includes most dial-up modem services, AOL broadband, some DSL services and others. If you have this type of connection, checking the **"I use dial-up..."** box will cause NOD32 to check for updates as soon as your Internet connection is established. (Recommended)

If you connect through a proxy server, select that option here also. If you don't know if you use a proxy server, you probably don't. In any case, selecting the **"I don't know..."** option is usually the safest, since it configures NOD32 to use the same settings as Internet Explorer.

## 1.6 Resident Scanner

The final setup screen (in the Typical installation) is the resident scanner startup configuration. AMON, the resident (or on-access) scanner, is the most crucial module of the NOD32 antivirus system. If another antivirus program

has previously been installed on your system, its resident (or on-access) scanner may conflict with NOD32's AMON. Usually, resident scanners will display an icon in the system tray (the area of the taskbar near the system




clock). We recommend removing any other antivirus software (including older versions of NOD32) before installing NOD32, version 2, to avoid serious problems.

If you're sure that no other antivirus scanner is running, check the **"Yes, I want to launch resident protection automatically"** box. This is important because the resident scanner (AMON) is the crucial module for preventing infection of your computer.


**IMPORTANT!** Running two resident (or "on-access") scanners is especially dangerous on Windows NT/2000/XP systems. Under Windows 95/98/Me it's a bit less dangerous, but we still recommend against running more than one resident scanner on a computer. Since the danger on a 95/98/Me PC is lower, the automatic protection box on the setup screen above is checked, by default, on Windows 95/98/Me systems, and unchecked on NT/2000/XP systems.

**NOTE:** If you are not sure about this matter, leave this box unchecked. After finishing the installation you can remove the other resident scanner. It is then very important to configure AMON to start automatically at system startup. To do this: Click on the **NOD32 Control Center** icon in the system tray (the white-green icon shown in the picture). Under **Resident Modules and Filters,** select **AMON**, click **Setup.** Click to select the **Security tab,** then check the box marked **"Enable automatic startup of AMON".**

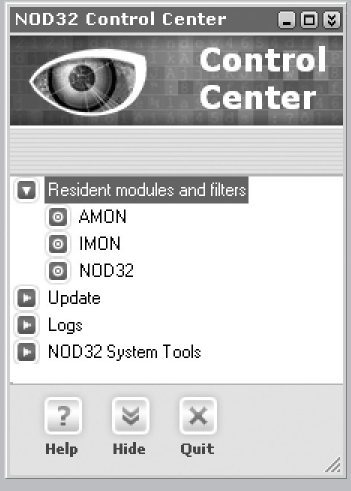

Click **Next,** and if you're satisfied with your settings, click **Next** again. Installation will complete, and you will be prompted to restart your computer. Click **Finish** to restart and begin protecting your computer with NOD32.

# 2 • Things to do after a new installation:

## 2.1 Make sure it's running


You should see an icon like this in the system tray:

That lets you know NOD32 is running. Click it once to bring up the following window:

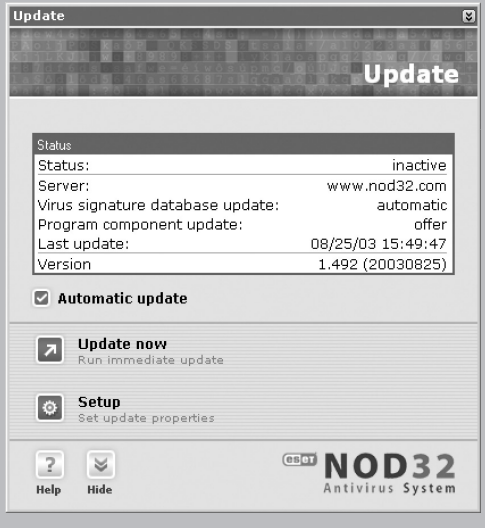


This is the NOD32 Control Center. From here you can control all aspects of NOD32's modules.

**NOTE:** The EMON module is designed to work with Microsoft Outlook, installed in Corporate Mode. If you do not use Outlook, or have installed it as an Internet-only mail client, you will not need the EMON module, so it will not be installed or visible in the Control Center. IMON will protect your POP3 mail in this case.

## 2.2 Make sure the database is up-to-date

In the Control Center (above), click on **"Update"**. This window will open to the right of the Control Center window:



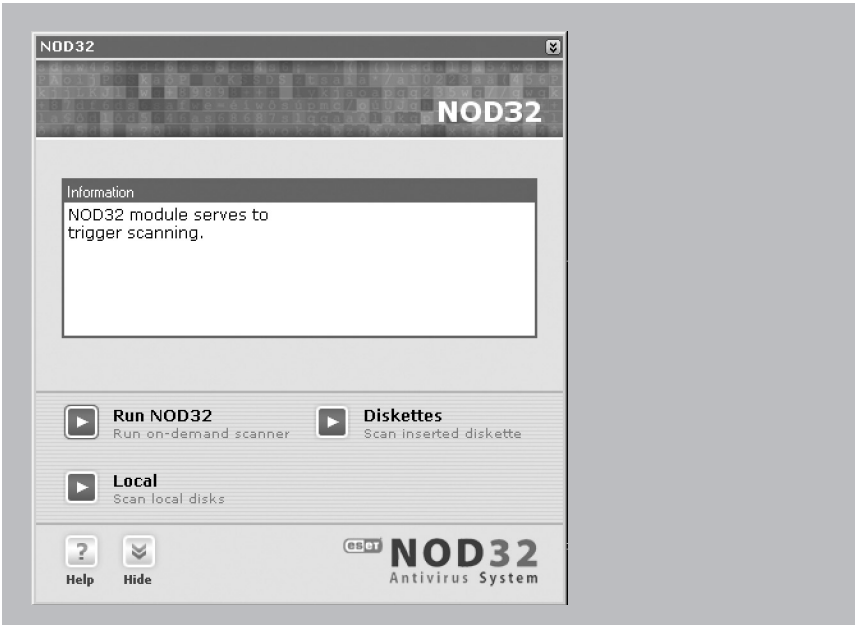

Ensure that the **Automatic update** box is checked, and click **Update now.**

If a dialog box pops up asking for your username and password, it's either because they were entered incorrectly during installation, or else your license has expired. Click **Setup** on this screen to re-enter your username and password as sent to you by your vendor.

**NOTE:** Both Username and password are case-sensitive, and must be entered exactly, including the dash "-" character in the username. We recommend using copy and paste.

## 2.3 Scan the system

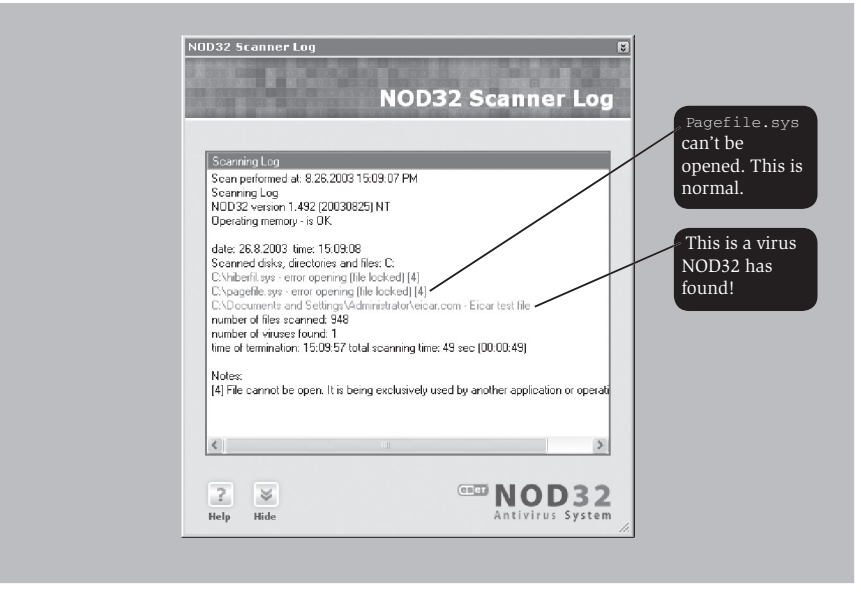
In the Control Center's left panel, select **"NOD32"** under the **"Resident modules and filters"** section. In the window that appears to the right, click




the **Local** button. This will start a scan of your system to catch and infections that might already be there. NOD32's advanced detection methods may find things your old scanner missed.

If your computer runs Windows NT, 2000, or XP, you may notice that one or two files can't be opened during the scan. Under normal conditions, `pagefile.sys` and `hiberfil.sys` cannot be opened for scanning because they are in use by the operating system. The first file is part of

the memory system, and so is scanned during the memory check that NOD32 does automatically when it first starts. The second file is part of the hibernation system, and gets overwritten whenever you use the hibernate



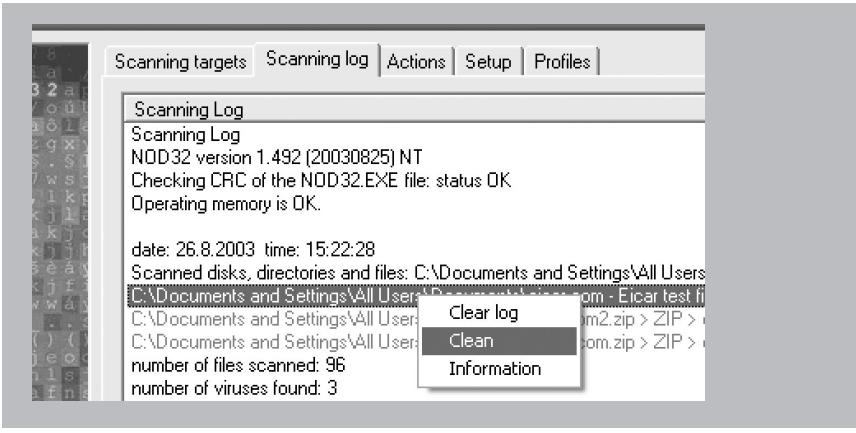

shutdown option. So for these two files, this is perfectly normal, and does not indicate a problem with your PC. (You won't see `hiberfil.sys` on NT at all, and only on 2000/XP systems that have hibernation enabled.)

But what about that virus? Read on...

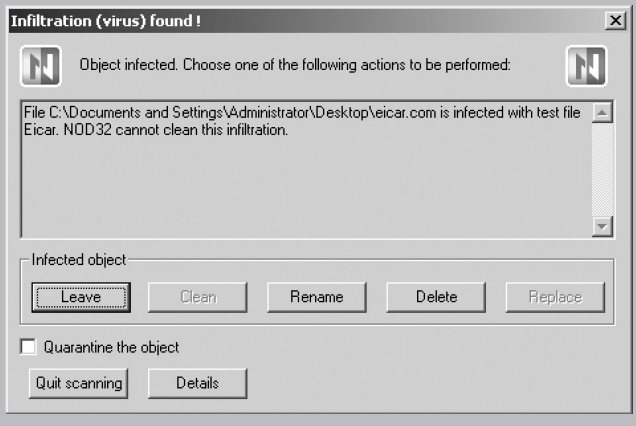
# 3 • What happens if I find a virus?

## 3.1 During on-demand (NOD32) scanning:

During a regular scan using NOD32, you may see virus detection warnings like the one here. These show up as a red entry in the scanning log, showing the name and path of the file, and the name of the infection. To handle these, simply right-click with your mouse on the log entry, and select **"clean"** from the pop-up menu:



A screen like this appears:




In this case the infected file is not recoverable, or didn't contain any data except the virus itself. This is quite common with modern email-borne "worms", and the solution is to simply rename or delete the infected file.

**IMPORTANT!** Before deleting a file make sure it does not contain any useful data and is not part of the operating system. If you're not sure, contact NOD32 Technical Support for assistance.

**NOTE:** If the name of the infection is "unknown" or "probable...", check the Quarantine box before cleaning or deleting the file. You can then follow the instructions for sending a sample of the suspicious file to our labs for analysis. *(See "Appendix C: Sending Virus Samples to Eset's labs" for more information)*

## 3.2 During regular computer use:

The NOD32 antivirus system is constantly on the lookout for new infections trying to enter your system during normal computer use. This keeps your system from getting infected. Virus warnings during times when you're not running a specific scan generally come from one of the NOD32 "on-access" modules: AMON (file access), IMON (POP3 email access), or EMON (MAPI email access, i.e. Microsoft Outlook in corporate mode).

These pop-up warnings are hard to miss:

As with the on-demand scanner, the options for dealing with an infection are **Clean, Delete,** and **Rename,** with an option to quarantine a copy of


the infected file first. Here again, files that cannot be cleaned can usually be deleted as they contain no useful data.

**IMPORTANT!** Before deleting a file make sure it does not contain any useful data and is not part of the operating system. If you're not sure, contact NOD32 Technical Support for assistance.

**IMPORTANT!** If the infected file cannot be cleaned, renamed, or deleted within the on-access scanner warning window (AMON, IMON, or EMON), please scan the system with NOD32 (the on-demand scanner as described in section "2.3 Scan the system". It may also help to put the computer in safe mode for this scan. (Press the F8 key during system startup and select „Safe mode").

**NOTE:** If the name of the infection is "unknown" or "probable...", check the Quarantine box before cleaning or deleting the file. You can then follow the instructions for sending a sample of the suspicious file to our labs for analysis. *(See Appendix C for more information)*

# Appendix A: **Troubleshooting**

**Q: My username or password doesn't work**

**A:** If a dialog box pops up asking for your username and password, it's because they were entered incorrectly during installation, or your NOD32 license has expired. If your license is up-to-date, click Setup on this screen to re-enter your username and password as sent to you by your vendor.

**NOTE:** Both Username and password are case-sensitive, and must be entered exactly, including the dash "-" character in the username. We recommend using "copy" & "paste" to enter these values.

If you have tried all these suggestions without success, please contact NOD32 Technical Support.

**Q: I get the message:** `"Microsoft Outlook. Either there is no default mail client or the current mail client cannot fulfill the messaging request. Please run Microsoft Outlook and set it as the default mail client."` **What is the problem?**

**A:** ***Overview:*** This message box is displayed by Microsoft Outlook when NOD32 tries to access MAPI32.DLL and Outlook is not the default mail client.

***Options:***

1. ***If you use Microsoft Outlook*** as your main program for receiving email and it is not set up as your default mail client, you can make it the default mail client in this way: In Internet Explorer, select **Tools → Internet Options → Programs → E-mail**, and change the default application to Microsoft Outlook.

2. ***If you have Microsoft Outlook installed but don't use it:*** Consider uninstalling it.

3. ***If you use Microsoft Outlook, but don't want it as your default email client:*** You can prevent NOD32 from accessing MAPI32.DLL. From the NOD32 Control Center, select **Resident modules and filters → NOD32** and launch the NOD32 on-demand scanner. In the **Setup** tab, clear the checkbox marked **"Use MAPI Interface"** in the system section.

**Q: Can I use NOD32's IMON with email client X?**

**A:** If your mail client uses the POP3 protocol, it will most likely work with IMON without any further configuration. Note that if you use IMAP or another protocol currently not supported by IMON, you are still protected from opening unsafe attachments by the AMON module.

———

Other questions? Start with the complete list of Frequently Asked Questions (FAQ) at

**`http://www.nod32.com/support/faq.htm`**.

If you don't find the solution there, please contact NOD32 Technical Support at

**`http://www.nod32.com/support/support.htm`**

# Appendix B: **Installation Types**

At the beginning of the installation process, there are three options for installation type: **Typical, Advanced,** and **Expert.** The difference between these is in which options are set to their default (and recommended) values, and which are presented as choices to the user. The following table summarizes the installation types:

| Option | Default | Typ. | Adv. | Exp. |
|---|---|---|---|---|
| NOD32 destination folder | C:\Program Files\Eset | | ● | ● |
| Silent Mode, password protect settings | No | | ● | ● |
| GUI type, Splash screen | Full graphic, Yes | | | ● |
| Send warnings by e-mail or messenger | No | | | ● |
| Update-server, username and Password | -none- | ● | ● | ● |
| Internet connection and proxy settings | -none- | ● | ● | ● |
| Auto-update configuration | Hourly or on-connect | | ● | ● |
| Launch resident protection on startup | Win9x: Yes, NT/XP: No | ● | ● | ● |
| Place icon on desktop | Yes | | ● | ● |
| Enable Explorer context-menu scanning | Yes | | ● | ● |
| Enable IMON and EMON, modification of infected mail, and appending notices to e-mail | Yes | | ● | ● |


**NOTE:** Most of these settings (and many others) can be (re-) configured after NOD32 is installed, no matter which installation type is chosen. Exceptions are: “Enable Explorer context-menu scanning” and “Place icon on desktop”, which are only available during initial installation.

# Appendix C: **Sending Virus Samples to Eset's labs**

Occasionally, you may get a virus alert where the name of the infection is "unknown" or "probable...". This is because one of the NOD32 modules has detected virus-like characteristics in a file, but doesn't have a matching signature to verify the virus name. This is most common with very new infections which have not yet been identified.

NOD32 has an impressive record of catching still-unknown, new viruses and worms because of the sensitivity and power of these "characteristic" scanning techniques, also known as *heuristics*. Since these are very often as-yet-unknown *malware* (bad software), we are very interested in receiving samples of these files for analysis.

To send Eset a sample, first check the **Quarantine** box before cleaning, renaming, or deleting the suspect file. The quarantine process saves a copy of the file in an encrypted and non-executable form, so no-one will be accidentally infected while moving the file, or sending it via email. The quarantined files are (by default) saved to "C:\Program Files\ESET\infected\". Each infection stored is stored in two parts, one ending in .NQF, the other ending in .NQI. The name of the quarantined files are generated randomly - if you have a number of such files in your "infected" folder, you may have to look at the creation date to determine which files are the ones you just saved. Do this by right-clicking on the file and selecting **Properties.** Email both parts to **samples@eset.com.**

# Appendix D: **Other Sources of Information**

Frequently Asked Questions (FAQ) at

**http://www.nod32.com/support/faq.htm**

On-line version of this manual, Admin Guide, and other documentation:

**http://www.nod32.com/download/manual.htm**

Nearest value added reseller (distributor):

**http//www.nod32.com/partners/partners.htm**

# Index

## S



## U



## V



## W

Part # ND2A-ENWNUG-01